AMENDEMENTS TO THE CLAIMS

1.   (Currently amended) An apparatus for managing access to a resource over a network, comprising:

        a transceiver arranged to receive a request for access to the resource from a client device; and

        an integrity management component, coupled to the transceiver, that is arranged to perform actions, including:

            providing a component to the client device;

            employing the component to gather integrity information associated with the client device, wherein the integrity information is gathered at a plurality of times;

            forwarding the integrity information to the apparatus;

            applying a dynamic policy for access to the resource based, in part, on the forwarded integrity information; and

            if the applied policy indicates a change in an integrity of the client device, performing a response based, in part, on the applied policy.

2.   (Original) The apparatus of claim 1, wherein the policy is manageable through a user interface at the apparatus.

3.   (Original) The apparatus of claim 1, wherein the integrity information further comprises an indicator that at least one of an antivirus product is enabled on the client device, a network sniffer is enabled, a screen scraper is enabled, a cracker tool is enabled, a hacker tool is

enabled, a firewall is enabled, a security application is enabled, and a client certificate is available on the client device.

4.   (Original) The apparatus of claim 1, wherein the integrity information further comprises a version indicator associated with at least one of an application, a process, and an operating system.

5.   (Original) The apparatus of claim 1, wherein the integrity information further comprises at least one of information associated with a process currently enabled on the client device, information associated with a sequence of system calls, and whether a predetermined file has been modified.

6.   (Original) The apparatus of claim 1, wherein the integrity information is gathered at a predetermined rate comprising at least one of a periodic rate, a random rate, and an aperiodic rate.

7.   (Original) The apparatus of claim 1, further comprising:
        sending a query request to the client device for selected information about the integrity of the client device.

8.   (Currently amended) The apparatus of claim 1, wherein ~~forwarding~~ the <u>forwarded</u> integrity information ~~further comprises at least one of compressing, and encrypting the integrity information~~ <u>comprises at least one of compressed or encrypted integrity information</u>.

9.   (Original) The apparatus of claim 1, wherein the performed response further comprises at least one of denying access to the resource, terminating a connection, and restricting access to the resource.

10.   (Original) The apparatus of claim 1, wherein the performed response further comprises providing a higher level of access to the resource.

11.　　(Original) The apparatus of claim 1, wherein at least some of the integrity information is gathered in response to a predetermined event.

12.　　(Original) A method of managing access to a resource over a network, comprising:

receiving a request for access to the resource from a client device;

receiving a first integrity information associated with the client device;

evaluating one or more policies for access based, in part, on the first integrity information;

receiving a second integrity information associated with the client device;

evaluating one or more policies for access based, in part, on the second integrity information; and

performing a response based, in part, on a difference between the first integrity information and the second integrity information.

13.　　(Original) The method of claim 12, wherein the performed response further comprises providing a higher level of access to the resource.

14.　　(Original) The method of claim 12, wherein the difference between the first integrity information and the second integrity information further comprises a change in antivirus security.

15.　　(Original) The method of claim 12, wherein the difference between the first integrity information and the second integrity information further comprises a change in a software configuration.

16.　　(Original) The method of claim 12, further comprising:

sending a request for the second integrity information to the client device, based, in part, on an event external to the client device.

17.   (Original) The method of claim 12, wherein the performed response further comprises maintaining a connection with the client device and providing a lower level of access to the resource.

18.   (Original) A method of managing access to a resource over a network, comprising:

receiving a request for access to the resource from a client device;

receiving a first integrity information associated with the client device at a first time;

receiving a second integrity information associated with the client device at a second time; and

performing a response based, in part, on a difference between the first integrity information and the second integrity information.

19.   (Original) The method of claim 18, wherein the first time and second time further comprises a time difference that is selected from at least one of a periodic rate, a random rate, and an aperiodic rate.

20.   (Original) The method of claim 18, wherein the first integrity information and the second integrity information further comprises an indicator that at least one of an antivirus product is enabled on the client device, that a network sniffer is enabled, a screen scraper is enabled, a cracker tool is enabled, a hacker tool is enabled, a firewall is enabled, a security application is enabled, and an indicator that the client device is enabled for a client certificate.

21.   (Original) The method of claim 18, wherein the first integrity information and the second integrity information further comprises a version indicator associated with at least one of an application, a process, and an operating system.

22.   (Original) The method of claim 18, wherein the performed response further comprises providing a higher level of access to the resource.

23.   (Original) The method of claim 18, wherein the performed response further comprises restricting access to the resource.

24.   (Original) The method of claim 18, wherein the difference between the first integrity information and the second integrity information further comprises a change in a security configuration.

25.   (Original) A system for managing access to a resource over a network, comprising:
        a client device configured to request access to the resource; and

        a server, coupled to the client device, that is configured to perform actions, including:

        receiving the request for access from a client device;

        providing a component to the client device;

        employing the component to gather integrity information associated with the client device, wherein the integrity information is gathered at a predetermined rate;

        receiving the integrity information at the predetermined rate from the component;

        applying a dynamic policy for access based, in part, on the forwarded integrity information; and

if the applied policy indicates a change in an integrity of the client device, performing a response based, in part, on the applied policy.

26.   (Original) The system of claim 25, wherein the integrity information further comprises at least one of information associated with a process currently executing on the client device, information associated with a sequence of system calls, and information indicating whether a predetermined file has been modified.

27.   (Original) The system of claim 25, wherein the predetermined rate further comprises at least one of a periodic rate, a random rate, an aperiodic rate, and being based on a predetermined event.

28.   (Currently amended) A computer-readable storage medium having a modulated data signal stored thereon for managing access to a resource over a network, the modulated data signal comprising operable to perform the actions of:

sending, from a client device, a request for access to the resource;

receiving, by a server, the request for access;

providing a component to the client device;

forwarding, towards the server, integrity information associated with the client device, wherein the integrity information is forwarded at a predetermined rate;

applying a dynamic policy for access to the resource based, in part, on the forwarded integrity information; and

if the applied policy indicates a change in an integrity of the client device, performing a response based, in part, on the applied policy.

29.   (Currently amended) The computer-readable storage medium of Claim 28, wherein the modulated data signal of claim 28, is further operable to perform the action of comprising: sending a query request to the client device for selected information about the integrity of the client device.

30.   (Currently amended) The computer-readable storage medium of Claim 28 modulated data signal of claim 28, wherein the predetermined rate further comprises at least one of a periodic rate, a random rate, an aperiodic rate, and a rate based on a predetermined event.

31.   (Original) An apparatus for managing a secure communication access over a network, comprising:

        a transceiver arranged to repeatedly receive integrity information reports at different times; and

        a means for modifying the secure communication access based, in part, on at least one difference between at least two of the integrity information reports.

32.   (Original) The apparatus of claim 31, wherein the means for modifying the secure communication access is configured to maintain the secure communication access and to reduce a level of access corresponding to the secure communication access.

33.   (Original) The apparatus of Claim 31, wherein the means for modifying the secure communication access is further configured to maintain the secure communication access and to increase a level of access corresponding to the secure communication access.

34.   (Original) The apparatus of claim 31, wherein the means for modifying the secure communication access is further configured to permit access to a first application at a remote server to be unchanged and to modify a level of access to a second application at the remote server.

35.   (Original) The apparatus of claim 31, further comprising logic for enabling the secure communication access through a virtual private network over a secure sockets layer.

36.   (Original) The apparatus of claim 31, further comprising logic for enabling the secure communication access through a virtual private network employing Internet Protocol Security (IPSec).

37.   (Original) A method of maintaining a secure communication access with a client device on a network, comprising:

establishing a level of access to one or more resources over a secure communication connection;

monitoring the client device for one or more changes to a security of the client device; and

selectively modifying the level of access to the one or more resources based on the one or more changes to the security of the client device.

38.   (Original) The method of claim 37, further comprising:

if the one or more changes to the security of the client device includes a change in software executing on the client device, providing a lower level of access to the one or more resources.

39.   (Original) The method of claim 37, further comprising:

if the one or more changes to the security of the client device includes a change in software executing on the client device, increasing the level of access to the one or more resources.